

Publication number: JP10512428 (T)

Publication date: 1998-11-24

- **international:** H04H1/00; H04H1/02; H04L9/00; H04N5/765; H04N5/92; H04N7/16; H04N7/167; H04N7/173; H04H1/00; H04H1/02; H04L9/00; H04N5/765; H04N5/92; H04N7/16; H04N7/167; H04N7/173; (IPC1-7): H04H1/00; H04H1/02; H04L9/00; H04L9/10; H04L9/12; H04N5/765; H04N5/92; H04N7/16; H04N7/173

Application number: JP19960517183T 19961023

Priority number(s): EP19950202980 19951031; WO1996IB01137 19961023

Abstract not available for JP 10512428 (T)

Abstract of corresponding document: WO 9716924 (A1)

Translate this text

In a conditional access system, transmitted information is recorded in a scrambled form (SV). Accordingly, any access to the recorded information (SV) is subject to the condition that proper control word(s) (CW) are available. To enable access to the recorded information (SV), control word regeneration data (ECM, KRD) is stored. The proper control word(s) (CW) cannot easily be derived from this control word regeneration data (ECM, KRD). However security device (SCD) is capable of retrieving the proper control word(s) (CW) from the control word regeneration data (ECM, KRD). A system operator effectively masters operations carried out in the security device (SCD). Accordingly, if the system operator so desires, he may inhibit retrieval of the control word(s) (CW) and, consequently, prevent access to the recorded information (SV). The conditional access system may be used in, for example, pay-TV or multimedia purposes.

特表平10-512428

(43) 公表日 平成10年(1998)11月24日

(51) Int.Cl. ⁴	識別記号	F I	
H 0 4 N	7/16	H 0 4 N	7/16 Z
H 0 4 H	1/00	H 0 4 H	1/00 F
	1/02		1/02 F
H 0 4 L	9/00	H 0 4 N	7/173
	9/10		5/92 H
審査請求 未請求 予備審査請求 未請求(全 25 頁) 最終頁に続く			

(21) 出願番号 特願平9-517183
 (86) (22) 出願日 平成8年(1996)10月23日
 (85) 翻訳文提出日 平成9年(1997)6月30日
 (86) 国際出願番号 P C T / I B 9 6 / 0 1 1 3 7
 (87) 国際公開番号 W O 9 7 / 1 6 9 2 4
 (87) 国際公開日 平成9年(1997)5月9日
 (31) 優先権主張番号 9 5 2 0 2 9 8 0 . 9
 (32) 優先日 1995年10月31日
 (33) 優先権主張国 オランダ (NL)
 (81) 指定国 EP (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), JP, KR

(71) 出願人 フィリップス エレクトロニクス ネムローゼ フェンノートシャップ
 オランダ国 5621 ベーアー アイन्दール
 フェン フルーネヴァウツウェッハ 1
 (72) 発明者 カンベルマン フランシスカス ルーカス
 アントニス ヨハネス
 オランダ国 5656 アーアー アイन्दール
 フェン プロフ ホルストラーン 6
 (74) 代理人 弁理士 杉村 曉秀 (外6名)

(54) 【発明の名称】 時間シフト限定アクセス

(57) 【要約】

限定アクセスシステムにおいて、送信された情報を、スクランブルされた形態 (SV) において記録する。したがって、記録された情報 (SV) に対するどのようなアクセスも、適切な制御ワード (CW) が利用可能な状態を条件とする。記録された情報 (SV) へのアクセスを可能にするために、制御ワード再生データ (ECM, KRD) を格納する。適切な制御ワード (CW) を、この制御ワード再生データ (ECM, KRD) から容易に得ることはできない。しかしながら、安全装置 (SCD) は、正確な制御ワード (CW) を制御ワード再生データ (ECM, KRD) から復元することができる。システムオペレータは、安全装置 (SCD) において行われる動作を実際に管理する。したがって、システムオペレータが望むなら、彼は、制御ワード (CW) の復元を禁止することができ、結果として、記録された情報 (SV) へのアクセスを防止することができる。本限定アクセスシステムを、例えば、有料TVまたはマルチメディア用途に用いることができる。

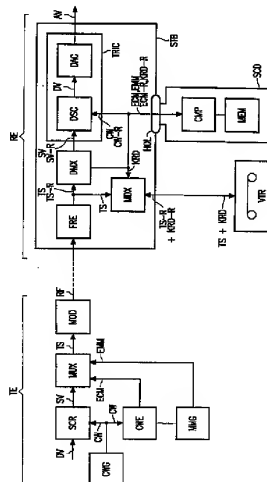


FIG. 1

【特許請求の範囲】

1. スクランプルされた情報（SV）を制御ワード（CW）に応じてデスクランブルされた情報（DV）に変換するデスクランブラ（DSC）と、

前記デスクランブラ（DSC）への前記制御ワード（CW）の供給を管理する安全装置（SCD）とを具える限定アクセスシステムにおいて、

該限定アクセスシステムが、前記制御ワード（CW）と等しくない制御ワード再生データ（KRD、ECM）を、スクランブルされた情報（SV）の記録に関連して格納媒体（VTR）に供給する手段（CMP、MEM）を具え、前記安全装置（SCD）が、

前記記録されたスクランブルされた情報（SV-R）の前記デスクランブラ（DSC）への供給に関連して、前記格納媒体（VTR）から読み出した制御ワード再生データ（KRD-R、ECM-R）から制御ワード（CW-R）を復元する手段（CMP、MEM）を具えることを特徴とする限定アクセスシステム。

2. 請求の範囲1に記載の限定アクセスシステムにおいて、前記制御ワード再生データ（KRD、ECM）を供給する手段（CMP、MEM）を、前記安全装置（SCD）に結合したことを特徴とする限定アクセスシステム。

3. 請求の範囲1に記載の限定アクセスシステムにおいて、前記安全装置（SCD）を、前記制御ワード再生データを供給する手段（CMP、MEM）を制御する権利情報を受けるように結合したことを特徴とする限定アクセスシステム。

4. 請求の範囲1に記載の限定アクセスシステムにおいて、前記安全装置（SCD）を、前記制御ワードを復元する手段（CMP、MEM）を制御する権利情報を受けるように結合したことを特徴とする限定アクセスシステム。

5. 請求の範囲1に記載の限定アクセスシステムにおいて、前記安全装置（SCD）を分離可能とし、該システムが、前記分離可能な安全装置（SCD）を保持するホルダ（HOL）を含むことを特徴とする限定アクセスシステム。

6. 制御ワード（CW）に応じてスクランブルされた情報（SV）をデスクランブルされた情報（DV）に変換するデスクランブラ（DSC）への前記制御ワ

ード（CW）の供給を管理する安全装置（SCD）において、該安全装置がさら

に、

前記制御ワード（CW）と等しくない制御ワード再生データ（KRD，ECM）を供給する手段（CMP，MEM）と、

前記制御ワード再生データ（KRD，ECM）から前記制御ワード（CW）を復元する手段（CMP，MEM）とを具えることを特徴とする安全装置（SCD）。

7．スクランブルされた情報（SV）と、

前記スクランブルされた情報（SV）をデスクランブルする、制御ワード動作されるデスクランブラ（DSC）において使用するために、制御ワード（CW）の復元を可能にする制御ワード復元データ（KRD，ECM）とを具える記録媒体。

8．デスクランブラ（DSC）によって制御ワード（CW）に応じてデスクランブルされた情報（DV）に変換することができる送信されたスクランブルされた情報（SV）の時間シフトされた限定アクセスの方法において、

前記スクランブルされた情報（SV）を記録するステップと、

前記制御ワード（CW）と等しくない制御ワード再生データ（KRD，ECM）を格納媒体（VTR）に供給するステップと、

記録されたスクランブルされた情報（SV-R）を前記デスクランブラ（DSC）に供給するステップと、

前記格納媒体（VTR）から制御ワード再生データ（KRD，ECM）を読み出すステップと、

前記デスクランブラ（DSC）に供給するために、前記制御ワード再生データ（KRD，ECM）から前記制御ワード（CW）を復元するステップとを具える方法。

9．請求の範囲1に記載の限定アクセスシステムにおける送信の方法において、記録権利情報を前記安全装置に送信することを特徴とする方法。

本発明は、

－ スクランブルされた情報を制御ワードに応じてデスクランブルされた情報に変換するデスクランブラと、

－ 前記デスクランブラへの前記制御ワードの供給を管理する安全装置とを具える限定アクセスシステムに係る。

このようなシステムを、例えば、テレビジョン放送において使用し、特定のテレビジョンチャネル、または番組のみを、これらのサービスに対して料金を支払った視聴者に対してアクセス可能にする、すなわち、有料TVを実現することができる。

1994年のSMPTE ジャーナルにおいて公表されたL.C.ギロウ (Guillou) およびJ.-L. ギアチェッティ (Giachetti) による記事“暗号化および限定アクセス”は、テレビジョン放送において使用する上述した形式の種々の限定アクセスシステムを記載している。既知のシステムにおいて、ビデオ信号をスクランブルされた形態において受信機に送信する。前記受信機は、デスクランブラを具え、このデスクランブラは、元のビデオ信号を復元するために前記送信信号をデスクランブルする。スクランブルおよびデスクランブルの双方を、制御ワードの制御の下で行う。使用するスクランブルアルゴリズムと共に前記制御ワードは、前記スクランブルされたビデオ信号と元のビデオ信号との関係を決定する。したがって、適切な制御ワードが利用可能ならば、前記スクランブルされたビデオ信号を、前記元のビデオ信号に変換し戻すことができるに過ぎない。したがって、受信端における前記元のビデオ信号へのアクセスは、前記制御ワードへのアクセスに制限される。

限定アクセスシステムの堅牢性を増すために、以下の手段を取る。第1に、前記制御ワードを定期的に変更する。第2に、前記制御ワードを、暗号化した形態において前記受信端に送信する。したがって、前記受信端は、前記元の制御ワ

ードを復元する暗号復号器を具える。第3に、前記暗号復号器を、復号を行うため

に入力データとして鍵を必要とするような方法において実現する。前記鍵と共に、前記暗号復号器が従って動作する復号アルゴリズムは、前記元の制御ワードと暗号化された制御ワードとの関係を決定する。

前記SMPTE 記事の図2ないし5は、前述の3つの手段を使用する限定アクセスシステムの例を示す。前記SMPTE 記事の図2において、管理メッセージと呼ばれる暗号化された制御ワードを、毎月郵便によって受信端に送る。前記受けた暗号化された制御ワードを復号するのに使用する鍵を、分配鍵とする。前記分配鍵は、受信端毎に異なる。このように、図2において、前記暗号化された制御ワードと、この暗号化された制御ワードを暗号復号化する鍵の双方を、個人化する。

前記SMPTE 記事の図3、4および5に示すシステムにおいて、暗号化された制御ワードと、この制御ワードを暗号復号化する鍵とを、個人化しない。例えば、前記スクランブルされたビデオ信号と共に、前記暗号化された制御ワードを権利制御メッセージ（ECM）の形態において送信することができる。これは、種々の受信端が、同じ暗号化された制御ワードを具える同じ権利制御メッセージECMを受信することを意味する。したがって、種々の受信端が、前記元の制御ワードを復元するのに同じ鍵を使用する。権利制御メッセージECMを復号する共通鍵を、許可鍵AKと呼ぶ。許可鍵AKおよび前記復号化アルゴリズムは、前記受信端における権利を表す。

許可鍵AKを、暗号化された形態において、権利管理メッセージ（EMM）として種々の受信端に送信する。受信端において、分配鍵を、権利管理メッセージEMMを暗号復号化するのに使用する。分配鍵を、代表的に多様化する、すなわち、これらを、受信端毎か、受信端のグループ毎に異ならせる。したがって、権利管理メッセージを個人化することができる。加えて、“マスタ”の声を認識するために、権利管理メッセージの確実性を受信端において検査すべきである。前記“マスタ”を、例えば、スクランブルされたビデオ信号の放送者であるサービス提供者と呼ぶ。

前記SMPTE 記事の図3、4および5のシステムにおいて、制御ワードは一般に極めて多数のビット（代表的に60ビット）と、短い寿命（代表的に10秒）と

を有する。これは、10秒毎に、権利制御メッセージECMの形態における新たな暗号化された制御ワードを、前記受信端に送信することを意味する。安全の理由のため、許可鍵AKを、その度毎に変更する。許可鍵AKを、暗号化された許可鍵AKを伝達する権利管理メッセージEMMによって更新する。

引用したSMPTE 記事に記載のシステムにおいて、各々の受信端は、安全装置を具える。前記安全装置は、受信端の権利に関する動作を行う、すなわち、有料TVオペレータコマンドを実行する。前記動作は、暗号化された制御ワードの暗号復号化と、適切ならば、権利管理メッセージEMMの暗号復号化とを含む。前記安全装置は、アクセスの権利を制限する状況に関係する他の動作を行ってもよい。このような状況は、例えば、予約期間、申込み前番組、一時的なアクセスに対する信用等である。

前記安全装置を、種々の方法において実現することができる。一般に、前記安全装置は、マイクロプロセッサを具える。前記安全装置を、前記デスクランブラに固定し、前記デスクランブラと集積し、1つのユニットを形成する。代わりに、前記安全カードをスマートカードとし、前記デスクランブラを具える受信ユニットから分離できるようにしてもよい。後者の選択は、前記制御ワードが多くビットと十分に短い寿命とを有する場合、十分に安全である。どのような実現においても、前記安全装置を、安全のために、物理的にまたは電子的に偽造できないようにするべきである。

本発明の目的は、前記システムオペレータに、前記送信された情報のアクセスのより広範囲な制御を与える、上述した形式の限定アクセスシステムを提供することである。

本発明のある態様によれば、このようなシステムは、該システムが、
— 前記制御ワードと等しくない制御ワード再生データを、スクランブルされた情報の記録に関連して格納媒体に供給する手段を具え、前記安全装置が、
— 前記記録されたスクランブルされた情報の前記デスクランブラへの供給に関連して、前記格納媒体から読み出した制御ワード再生データから制御ワードを復元する手段を具えることを特徴とする。

本発明の他の態様は、実際に、上記で規定した限定アクセスシステムに従っ

て、安全装置と、記録媒体と、時間シフト限定アクセスとに關係する。追加の特徴を、継続の請求の範囲において規定する。

本発明は、前記SMPTE 記事が行わない、情報を守る時間シフトアクセスの機能を考慮する。引用したSMPTE 記事に記載のすべての限定アクセスシステムは、情報への、この情報の送信の時間における許可されないアクセス、すなわち短く直接アクセスを防ぐことに焦点を置いている。しかしながら、権利を与えられた受信端において、前記デスクランブルされた情報を、例えばテープに記録することができる。前記有料TVオペレータは、前記記録された情報を実際に制御することができず、許可されない人物がこの記録された情報に自由にアクセスすることができる。

例えば、共同住宅において、スクランブルされたテレビジョン（TV）チャンネルに予約した住人は、このチャンネルにおける番組をデスクランブルされた形態において記録することができる。その後、彼は、この記録を、予約者ではないがこの番組を観たい他の住人に手渡すことができる。さらに、前記デスクランブルされた番組がダビング防止されていない場合、前記記録された番組による複製を物理的に防ぐことはできない。これらの複製を、例えば、その番組をいつでも好きなときに観るために前記關係するTVチャンネルに予約する必要があるような種々の住人に配布することができる。

デジタルテレビジョン放送の出現により、上述したことは有料TVオペレータにとってより大きな問題になる。番組を、例えばMP E G-2デジタルビデオ信号として放送し、この番組のMP E G-2デジタルビデオ信号を記録する場合、この記録は、前記放送とほぼ同じ画像および音声品質を与える。どのようなダビング防止法も外した場合、前記番組を、どのような意味のある品質の劣化もなく、隙限なく複製することができる。すなわち、有料TVシステムにおける各々の受信端は、放送された有料TV番組の海賊版マスタの潜在的なオーナーである。デジタル有料TVシステムにおいて、前記海賊版マスタは、前記有料TVオペレータの公認マスタと同じ位またはほとんど同じ位良好である。

本発明による限定アクセスシステムにおいて、前記放送された情報は、前記システムオペレータが望む場合、依然として彼の制御の下にある。例えば、前記シ

ステムオペレータは、前記記録された情報にアクセスできる回数、前記記録された情報にアクセスできる期間、前記記録された情報にアクセスできる受信端、等を決定することができる。このように、本発明は、時間シフト情報アクセス機能を前記既知の限定アクセスシステムに付加すると同時に、この機能がこれらのシステムの安全性に影響を及ぼすことを回避する。

本発明のこれらのおよび他の態様および利点は、以下に記載の実施例の参照によって明らかになるであろう。

図 1 は、本発明による限定アクセスシステムの一実施例のブロック図である。

図 2 a は、図 1 の限定アクセスシステムの第 1 の実現化における記録に関係する動作を説明する機能的な図である。

図 2 b は、図 1 の限定アクセスシステムの第 1 の実現化における再生に関係する動作を説明する機能的な図である。

図 3 a は、図 1 の限定アクセスシステムの第 2 の実現化における記録に関係する動作を説明する機能的な図である。

図 3 b は、図 1 の限定アクセスシステムの第 2 の実現化における再生に関係する動作を説明する機能的な図である。

図 4 a は、図 1 の限定アクセスシステムの第 3 の実現化における記録に関係する動作を説明する機能的な図である。

図 4 b は、図 1 の限定アクセスシステムの第 3 の実現化における再生に関係する動作を説明する機能的な図である。

本発明を、有料 TV システムにおける用途を用いてより詳細に説明する。第 1 に、図 1 に示す有料 TV の機能要素を論考する。第 2 に、図 1 の有料 TV システムの 3 つの実現化を論考し、これらの実現化においては、前記システムは異なつて動作する。図 2 a、2 b、図 3 a、3 b および図 4 a、4 b は、これら 3 つの個々の実現化における動作を説明する。第 3 に、本発明によって与えられる有料 TV システムにおける有利な効果を強調する。第 4 に、いくつかの代わりの実施例を取り扱い、請求した本発明の範囲が以下に例として与える有料 TV システムを十分に越えることを示す。

図 2 の有料 TV システムにおいて、送信端 TE は、有料 TV 番組をスクランブル

ルされた形態において、受信端REに伝送する。受信端REは、ビデオテープレコーダVTRを有し、どのような送信された有料TV番組も送信時より後の時間において観ることができる。これをさらに、時間シフトされた視聴と呼ぶ。前記受信端は、以下のユニット、すなわち、セットトップボックスSTBと、分離可能安全装置SCD、例えばスマートカードとをさらに具える。セットトップボックスSTBは、物理的および電氣的に安全装置SCDを結合するホルダHOLを有する。

送信端TEにおいて、スクランブル化装置SCRは、ビデオ信号DV、例えばMPEG-2符号化ビデオ信号をスクランブルし、スクランブルされたビデオ信号SVを得る。前記スクランブル化は、制御ワードCWに依存し、この制御ワードCWを制御ワード発生器CWGによって発生する。このために、デジタルビデオ信号DVとスクランブルされたビデオ信号SVとの関係は、制御ワードCWと使用されるスクランブル化アルゴリズムとによって決定される。制御ワード発生器によって与えられる制御ワードCWを、例えば、10秒毎に周期的に変化させる。

制御ワード暗号器CWEおよび管理メッセージ発生器MMGは、受信端REにおけるデスクランブル化に必要なデータを与える。さらに特に、制御ワード暗号器CWEは、制御ワードCWを暗号化した形態において与え、これらのワードを、権利制御メッセージECMに含める。管理メッセージ発生器MMGは、許可鍵AKを暗号化された形態において与え、この鍵を権利管理メッセージEMMに含める。許可鍵AKは、権利制御メッセージECMから制御ワードを復元するのに必要である。

権利制御メッセージECMは、少なくとも制御ワードCWにおける変化と同じくらい頻繁に変化する。例えば、10秒毎に、新たな制御ワードCWを具える権利制御メッセージECMが、前記受信端に伝送される。しかしながら、制御ワードCWをデスクランブルする許可鍵AKは、制御ワードCWよりかなり間を置いて、例えば、1週間または1か月に一度のみ変化する。したがって、権利管理メッセージEMMは、権利制御メッセージECMよりかなり頻度が少ない。したがって、テレビジョン番組中、例えば、多数の権利制御メッセージECMが受信端

REに伝送されるが、権利管理メッセージEMMはまったく伝送されない。

マルチプレクサMUXは、スクランブルされたビデオ信号SVと、権利制御メッセージECMおよび権利管理メッセージEMMとを、1つの輸送ストリームに結合する。輸送ストリームTSを変調器MODに供給し、変調器MODは、送信信号RFを与える。

受信端REにおけるセットトップボックスSTBは、以下の機能的部分、すなわち、フロントエンドFRE、デマルチプレクサDMX、マルチプレクサ/デマルチプレクサMDX、デスクランブラDSCおよびアナログーデジタル(A/D)コンバータADCを具える。フロントエンドFREは、送信信号RFから輸送ストリームTSを得る。輸送ストリームTSをデマルチプレクサDMXに供給し、このデマルチプレクサDMXは、輸送ストリームTSに含まれる種々の形式の情報を分離する。したがって、スクランブルされたビデオ信号SVは、権利制御メッセージECMおよび権利管理メッセージEMMから分離される。マルチプレクサ/デマルチプレクサMDXは、ビデオテーブルコーダVTRに対するインタフェースである。以下により詳細に論考する。

デスクランブラDSCは、スクランブルされたビデオ信号SVを受け、安全装置SCDから制御ワードCWを受ける。適切な制御ワードCWによって、デスクランブラDSCは、スクランブルされたビデオ信号SVをデジタルビデオ信号DVに変換し、このデジタルビデオ信号DVは、前記送信端においてスクランブラSCRに供給されたものである。デジタルーアナログ(D/A)コンバータDACは、デジタルビデオ信号DVを、画像表示装置(図示せず)に供給するのに適切なアナログビデオ信号AVに変換する。デスクランブラDSCおよびD/AコンバータDACを、偽造防止集積回路TRICに収容する。したがって、デジタルビデオ信号DVに容易にアクセスできないため、どのような有料TV番組のデジタル記録も妨げられる。

安全装置SCDは、デマルチプレクサDMXによって供給される権利制御メッセージECMおよび権利管理メッセージEMMを暗号復号化する。権利管理メッセージEMMの暗号復号化は、許可鍵AKを与え、この許可鍵AKは、権利制御メッセージECMおよび/または受信端REの権利に関する他のデータを暗号復

号化するのに必要である。権利制御メッセージECMの暗号復号化は、制御ワードCWを与え、この制御ワードCWは、デジタルビデオ信号DVを復元するためにデスクランブラDSCが必要とする。

安全装置SCDは、上述した動作を行い、その結果を格納する、マイクロコンピュータCMPおよびメモリMEMを見える。メモリMEMは、最新の権利制御メッセージECMから得られた現在の制御ワードCWを格納することができる書き込み可能部分を有する。さらに、権利制御メッセージECMを暗号復号化する許可鍵AKを、新たな権利管理メッセージEMMを受けるまで、前記書き込み可能部分に格納する。メモリMEMは、さらに、例えば、暗号復号化アルゴリズムを格納する読み出し専用部分を有してもよい。

ビデオテープレコーダVTRは、マルチプレクサ/デマルチプレクサMDXから、記録するための入力信号を受ける。この入力信号は、輸送ストリームTSを見える。このように、ビデオテープレコーダVTRは、スクランブルされた形態におけるどのような有料TV番組も、付随する権利制御メッセージと共にデジタル式に記録することができる。記録された有料TV番組を再生する場合、記録された輸送ストリームTS-Rを、マルチプレクサ/デマルチプレクサMDXを経てデマルチプレクサDMXに供給する。したがって、デマルチプレクサDMXは、記録された権利制御メッセージECM-Rを安全装置SCDに供給し、記録されたスクランブルされたビデオ信号SV-RをデスクランブラDSCに供給する。

しかしながら、輸送ストリームTSのみを記録した場合、記録された有料TV番組を観ようとする、以下の問題が生じる。記録された有料TV番組を再生する時間において、記録が行われた時間から権利管理メッセージEMMが安全装置SCDに伝送されてしまっているかもしれない。その場合において、記録の時間に変化する許可鍵AKは、新たな許可鍵AKに置き換えられている。結果として、安全装置SCDは、供給された記録された権利制御メッセージECM-Rから適切な制御ワードCWを復元することができない。

図1の有料TVシステムにおいて、安全装置SCDは、有料TV番組が記録された場合、鍵関連データKRDを与える。鍵関連データKRDを、マルチプレク

サ/デマルチプレクサMDXにおいて輸送ストリームTSに結合し、続いてビデオテープレコーダVTRに供給する。記録された有料TV番組を再生する場合、記録された鍵関連データKDR-Rは、マルチプレクサ/デマルチプレクサMDXを経て安全装置SCDに戻る。安全装置SCDは、鍵関連データKRDを使用して、前記記録の時間において変化した許可鍵を再インストールする。したがって、記録された権利制御メッセージECM-Rを暗号復号化することができ、結果として、前記記録に適合した制御ワードCW-Rを再生中にデスクランブラDSCに供給することができる。

図1の有料TVの、鍵関連データKRDが性質において異なる3つの実現化を以下に説明する。しかしながら、3つの実現化のすべては共通して、だれか許可されない人物が鍵関連データKRDから適切な許可鍵AKを得ることは、可能であっても困難である。

図2aおよび2bは、図1の有料TVシステムの第1の実現化における、安全装置SCDにおいて行われる動作を説明する。図2aにおいて、有料TV番組をその送信の時間において観るために必要な動作を、比較的細い線によって示す。安全装置SCDに伝送される権利管理メッセージEMMの暗号復号化DMMは、許可鍵AKを与える。許可鍵AKのメモリMEMへの書き込みWKTは、少なくとも新たな権利管理メッセージEMMが伝送されるまで、安全装置SCDにおいて許可鍵AKを利用可能にする。許可鍵AKのメモリMEMからの読み出しRKTによって、許可鍵AKを権利制御メッセージECMの暗号復号化DCMにおいて使用する。暗号復号化DCMは、図1に示すデスクランブラDSCにおけるスクランブルされたビデオ信号SVをデスクランブルするのに必要な適切な制御ワードCWを与える。

図2aにおいて、有料TV番組の記録に係るこれらの動作を、太線において示す。有料TV番組の記録の確認IRCは、許可鍵AKの暗号化EAKに関する条件であり、この鍵を、メモリMEMから読み出しRKEによって読み出す。暗号化された許可鍵E(AK)は、図1に示すような輸送ストリームTSと共にビデオテープレコーダVTRにおいて記録された鍵関連データKRDを構成する。記録された有料番組を再生する場合、図1における鍵関連データKRD-Rに

当する記録された暗号化許可鍵E（AK）－Rを、マルチプレクサ／デマルチプレクサMDXを経て安全装置SCDに供給する。

図2bは、記録された有料TV番組を観るために行われるこれらの動作を説明する。暗号復号化DAKは、暗号化された許可鍵E（AK）から記録許可鍵AK－Rを復元する。記録許可鍵AK－Rは、記録された有料TV番組の送信時においてメモリMEMにおいて存在する許可鍵AKに等しい。メモリMEMへの記録許可鍵AK－Rの書き込みWKRは、安全装置SCDにおいて記録許可鍵AK－Rを、少なくとも記録された有料TV番組の視聴が終了するまで利用可能にする。時間シフト視聴の確認ITSは、メモリMEMからの記録許可鍵AK－Rの読み出しRKRの条件である。記録RKRにより、記録許可鍵AK－Rを、記録された権利制御メッセージECM－Rの暗号復号化DCMにおいて使用する。図2bにおける暗号復号化DCMは、記録されたスクランブルされたビデオ信号TS－Rをデスクランブルする制御ワードCW－Rをあたえる。

図3aおよび3bは、図1の有料TVシステムの第2の実現化において、安全装置SCDにおいて行われる動作を説明する。図3aにおける比較的細い線による動作は、図2aにおけるこれらと同じである。図3aにおいて、許可鍵AKの複製CKTを、メモリMEMにおいて、有料TV番組の記録IRCの確認に応じて行う。したがって、複製された許可鍵AK－Cは、MEMにおいて存在する。許可鍵AKとは違って、複製された許可鍵AK－Cは、原則的には、新たな権利管理メッセージEMMが安全装置SCDに伝送された場合、上書きされない。ラベル発生LAGは、アドレスADを、複製された許可鍵AK－CをメモリMEMに格納するのに従って、ラベルLABに変換する。ラベルLABは、鍵関連データKRDを構成し、これは、図1において示すような輸送ストリームTSと共に記録されたものである。記録された有料TV番組を再生する場合、図1における記録された鍵関連データKRD－Rに等しい記録されたラベルLAB－Rを、マルチプレクサ／デマルチプレクサMDXを経て安全装置SCDに供給する。

図3bは、記録された有料TV番組の再生に関係する動作を説明する。ラベル

解釈LAIは、複製された確認鍵AKをメモリMEMに格納するのに従って、アドレスADを復元する。時間シフトされた視聴ITSの確認を条件として、複製

された許可鍵AK-Cの読み出しRKCを行う。読み出しRKCにより、複製された許可鍵AK-Cを、記録された権利制御メッセージECM-Rの暗号復号化DCMにおいて使用する。図3bにおける暗号復号化DCMは、制御ワードCW-Rを与え、これは、記録されたスクランブルされたビデオ信号SV-Rをデスクランブルするのに適切である。

図4aおよび4bは、図1の有料TVシステムの第3の実現化において、安全装置SCDにおいて行われる動作を説明する。図4aにおける比較的細い線による動作は、図2aにおけるこれらと同じである。図4aにおいて、安全装置SCDに伝送された権利管理メッセージEMMのメモリMEMへの書き込みWMMを行う。したがって、権利管理メッセージEMMを、安全装置SCDのメモリMEMに格納する。これは、標準的な慣習ではないことに注意されたい。通常、権利管理メッセージEMMの暗号復号化DMMの結果を格納し、この結果は許可鍵AKを具えるが、権利管理メッセージEMMそれ自身は格納しない。有料TV番組の記録の確認IRCの状態を条件として、メモリMEMに格納された権利管理メッセージEMMの読み出しRMMを行う。読み出しRMMにより、権利管理メッセージEMMを、鍵関連データKRDとして、図1に示すマルチプレクサ/デマルチプレクサMDXに供給し、結果として、権利管理メッセージEMMを、輸送ストリームTSと共に記録する。

図4bは、記録された有料TV番組を再生するために行う動作を説明する。有料TV番組の時間シフトされた視聴ITSの確認の状態を条件として、記録された権利管理メッセージEMM-Rの暗号復号化DMMを行う。暗号復号化DMMは、記録された権利管理メッセージEMM-Rから記録許可鍵AK-Rを復元する。図4bに示す他の動作は、図2bに示すこれらと同じである。

以下の意見は、3つの上述した実現化に関するものである。第1に、図2b、3bおよび4bに示す暗号復号化DCMは、図2a、3aおよび4aに示すこれらと、動作において同じである。これらを実行する瞬間、すなわち、関連した有

料ＴＶ番組の、各々、再生中か、送信中かのみが異なっている。

第２に、図２ a および ２ b と図４ a および ４ b とに各々示す第１および第３の実現化において、許可鍵ＡＫを、暗号化された形態において、安全装置ＳＣＤの

外部に格納する。前記第１の実現化において、許可鍵ＡＫを、安全装置ＳＣＤにおいて暗号化する。記録鍵を、許可鍵ＡＫを暗号化するのに使用することができ、この記録鍵を、安全装置ＳＣＤに固有のものとしてもよい。前記第３の実現化において、権利管理メッセージＥＭＭになる、送信端における許可鍵ＡＫの暗号化を有効に使用する。このように、図４ b に示す鍵関連データＫＲＤの暗号復号化ＤＭＭは、図４ a における暗号復号化ＤＭＭと同じである。

第３に、上述した実現化において記録することを権利に含め、どのような有料ＴＶ番組の記録も許可するまたは禁止するようにすることができる。例えば、安全装置ＳＣＤによる鍵関連データＫＲＤの出力を、受信端ＲＤが関連する有料ＴＶ番組を記録する権利を与えられる状態を条件として行うことができる。これは、送信の瞬時において有料ＴＶ番組を視聴する権利を除く、すなわち、時間シフトされた視聴のみが禁止される。例えば、送信端ＴＥは、記録権利を、直接の視聴権利と同様にすなわち、権利管理メッセージＥＭＭによって伝送することができる。

第４に、時間シフトされた視聴の表示ＩＴＳを、輸送ストリームＴＳにおける時間スタンプされたメッセージから得ることができる。例えば、権利管理メッセージＥＣＭが、このようなタイムスタンプされたメッセージを具えてもよい。したがって、時間チェック機能を、図１の有料ＴＶシステムに与える。安全装置ＳＣＤに内部クロックを設けた場合、直接視聴に関する輸送ストリームＴＳか、時間シフトされた視聴に関する輸送ストリームＴＳ－ＲかのどちらがセットトップボックスＳＴＢにおいて処理されているかを区別することができる。さらに、前記記録の年齢を決定することができ、この情報を使用して、視聴を許可するかまたは許可しないかを決定することができる。

第５に、輸送ストリームＴＳは、それが由来するところのものから有料ＴＶ番組を識別するデータを具えてもよい。例えば、権利制御メッセージＥＣＭは、ど

の有料TV番組がこれらの権利制御メッセージECMと多重化されているかを区別するデータを含んでもよい。この場合、安全装置SCDは、受けた権利制御メッセージECMから、どの有料TV番組がデスクランブラDSCに供給されているかを決定することができる。

上述した有料TVシステムにおいて用いた本発明は、有料TVオペレータが、実際に、記録された有料TV番組の“マスタ”であるという利点を与える。これは、有料TVオペレータが、彼がそう望む場合、記録された有料TV番組のどのような視聴も禁止できることを意味する。記録された有料TV番組を視聴するために必要な制御ワードCW-Rを、安全装置SCDにおいて、記録された権利制御メッセージECM-Rと、記録された鍵関連データKRD-Rとから復元する。前記TVオペレータは、安全装置SCDにおける動作を制御する者である。したがって、彼は、適切な制御ワードCW-RをデスクランブラDSCに供給するために満たされなければならない条件を与えてもよい。

例えば、有料TVオペレータは、以下の方法において、記録された有料TV番組を観ることが出来る回数を決定することができる。有料TVオペレータは、権利管理メッセージEMMを安全装置SCDに伝送し、条件“記録された有料TV番組の視聴は5回以下”を設定することができる。視聴の回数を計数するために、安全装置SCDは、番組識別および計数用ソフトウェアを具えてもよい。安全装置SCDが、有料TV番組が6回目の視聴であることを確立した場合、デスクランブラDSCへの制御ワードCW-Rの供給を禁止する。

有料TVオペレータが与えることができる他の条件は、有料TV番組を観ることが出来る期間である。再び、この条件を、権利管理メッセージEMMによって、安全装置SCDに伝送してもよい。安全装置SCDは、安全装置SCDに供給された番組の年齢を決定するソフトウェアを具えてもよい。例えば、権利制御メッセージECMに含まれる上述したタイムスタンプされたメッセージを、この目的のために使用することができる。

本発明は、さらに、原則的に、記録された有料TV番組を、記録に使用された安全装置SCDが利用可能な場合にのみ視聴することができるという利点を与え

る。輸送ストリームＴＳと共にテープに記録された鍵関連データＫＲＤのみが、この鍵関連データＫＲＤを発生した安全装置に対して意味がある。記録された有料ＴＶ番組を再生する場合、他の安全装置ＳＣＤが、鍵関連データＫＲＤから適切な許可鍵ＡＫを得る可能性は、除外されないとしても非常に成功しそうにない。したがって、図１に示す受信端ＲＥの所有者が、彼の友人にテープに記録された

有料ＴＶ番組を貸した場合、前記所有者が彼の安全装置ＳＣＤも彼の友人に貸した場合のみ、この友人は前記有料ＴＶ番組を観ることができる。前記所有者が彼の安全装置ＳＣＤを貸さない場合、問題の友人は、有料ＴＶオペレータに、彼に視聴する権利を与えることを要求しなければならない。

加えて、本発明は、記録された有料ＴＶ番組が版權保護されるという利点を与える。記録された有料ＴＶ番組のどのような複製も、オリジナルを記録するのに使用された安全装置が利用可能である場合にのみ観ることができることは、上記から明らかであろう。

まとめにおいて、本発明は、有料ＴＶシステムに時間シフトして視聴する機能を与え、同時にこの機能が前記有料ＴＶシステムの安全性に实际的に影響を及ぼすのを回避する。

例として与えたこれら以外の多数の実施例および実現化も、請求した本発明の範囲内であることは明らかであろう。

許可鍵ＡＫ以外の限定アクセスデータを、上述した実施例における許可鍵ＡＫと同様に処理することができる。このような限定アクセスデータは、例えば、一般的に指定される許可鍵ＡＫを、受信端ＲＥにおける権利付与に使用することの正当性に関係してもよい。図２ａを参照すると、権利付与を、鍵関連データＫＲＤおよび輸送ストリームＴＳを図１に示すビデオテープレコーダＶＴＲにおいて記録するために、安全装置ＳＣＤにおいて暗号化することができる。

機能的要素を種々のユニットへ物理的に分布させる多数の方法が存在する。図１は、極めて図式的であり、本発明による条件アクセスシステムの１つの可能な実施例を表しているに過ぎない。例えば、図１に示す条件アクセスシステムのす

すべての機能的要素を、ビデオテープレコーダVTRに統合してもよい。代わりの実施例において、安全装置SCDを、ビデオテープレコーダVTRから分離可能なスマートカードとして実現することができる。他の代わりの実施例において、安全装置SCDを、セットトップボックスSTBに統合してもよい。これらを、記録のための専用のユニットと、他の目的のための他のユニットとしてもよい。

鍵関連データKRDを輸送ストリームTSと共にビデオテープレコーダVTRにおいて格納する代わりに、鍵関連データKRDをどこか他に格納してもよい。

例えば、鍵関連データKRDを、セットトップボックスSTBに結合したメモリ（図示せず）に格納することができる。もちろん、この実施例において、セットトップボックスSTBに格納された鍵関連データKRDを記録された有料TV番組にリンクする設備を形成しなければならない。

ビデオテープレコーダVTRの代わりに、なにか他の記録媒体、例えば、光または磁気ディスクを使用してもよい。本発明を、別個のハードウェアによって、または適切なソフトウェアによって供給されるプロセッサによって実現することができる。請求の範囲におけるどのような参照符も、関連する請求の範囲を制限すると解釈すべきではない。限定アクセスシステムにおいて、送信された情報を、スクランブルされた形態SVにおいて記録する。したがって、記録された情報SVに対するどのようなアクセスも、適切な制御ワードCWが利用可能であるという状態を条件とする。記録された情報SVへのアクセスを可能にするために、制御ワード再生データECM、KRDを格納する。適切な制御ワードCWを、この制御ワード再生データECM、KRDから容易に得ることはできない。しかしながら、安全装置SCDは、制御ワード再生データECM、KRDから適切な制御ワードCWを復元することができる。システムオペレータは、安全装置SCDにおいて行われる動作を実際に管理する。したがって、システムオペレータがそ望むなら、彼は、制御ワードCWの復元を禁止することができ、したがって、記録された情報へのアクセスを防止することができる。

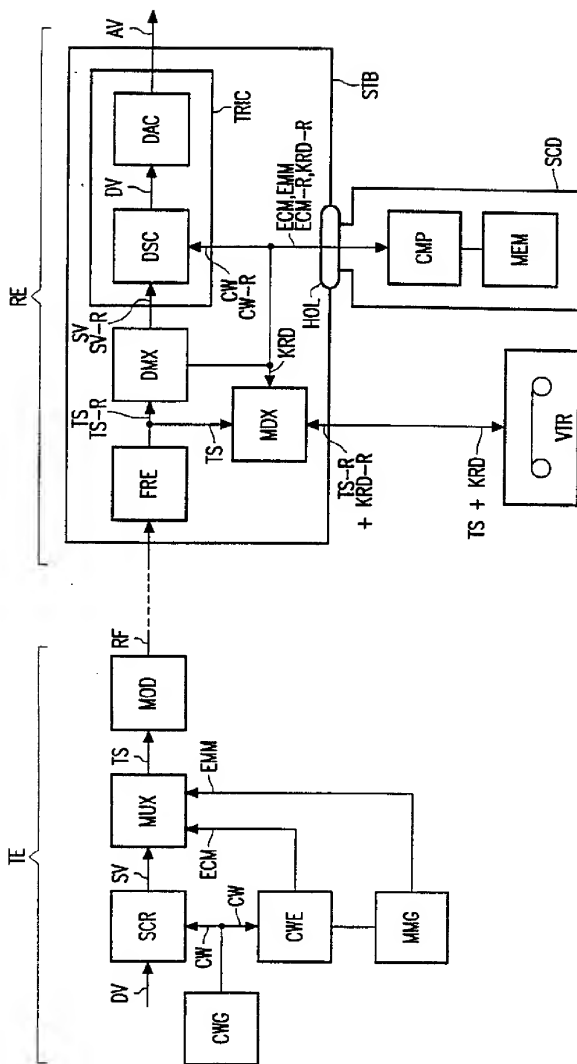


FIG. 1

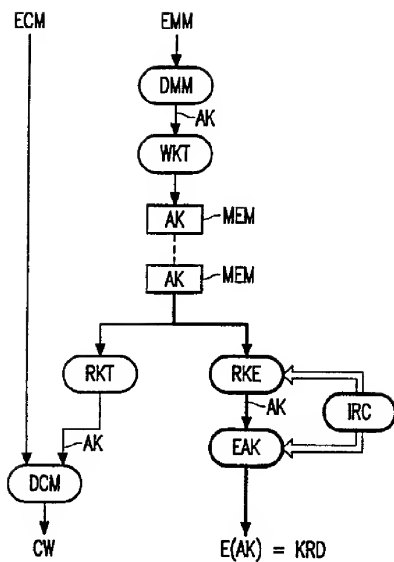


FIG. 2a

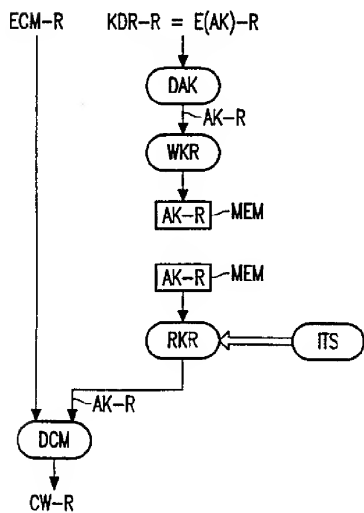


FIG. 2b

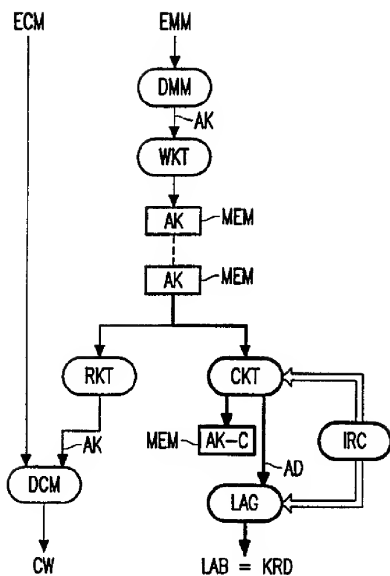


FIG. 3a

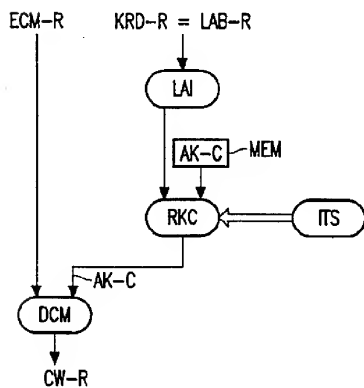
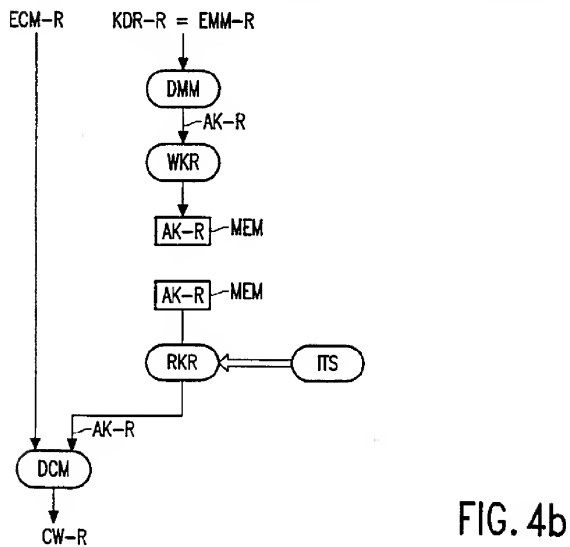
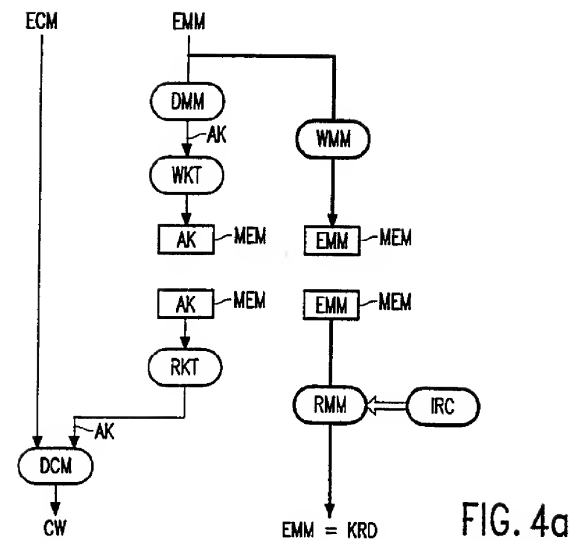


FIG. 3b



INTERNATIONAL SEARCH REPORT

International application No.

PCT/IB 96/01137

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04N 7/167, H04K 1/04

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04K, H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2132860 A (BRITISH BROADCASTING), 11 July 1984 (11.07.84), figure 1, abstract	1
A	---	2-5

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"Z" document member of the same patent family

Date of the actual completion of the international search

Date of mailing of the international search report

20 February 1997

21-02-1997

Name and mailing address of the ISA/

Authorized officer

Swedish Patent Office

Rune Bengtsson

Box 5055, S-102 42 STOCKHOLM

Telephone No. +46 8 782 25 00

Facsimile No. +46 8 666 02 86

Form PCT/ISA/210 (second sheet) (July 1992)

03/02/97

International application No.
PCT/IB 96/01137

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB-A- 2132860	11/07/84	NONE	

フロントページの続き

(51) Int. Cl. ⁶	識別記号	F I	
H O 4 L	9/12	H O 4 N	5/91 L
H O 4 N	5/765	H O 4 L	9/00
	5/92		Z
	7/173		